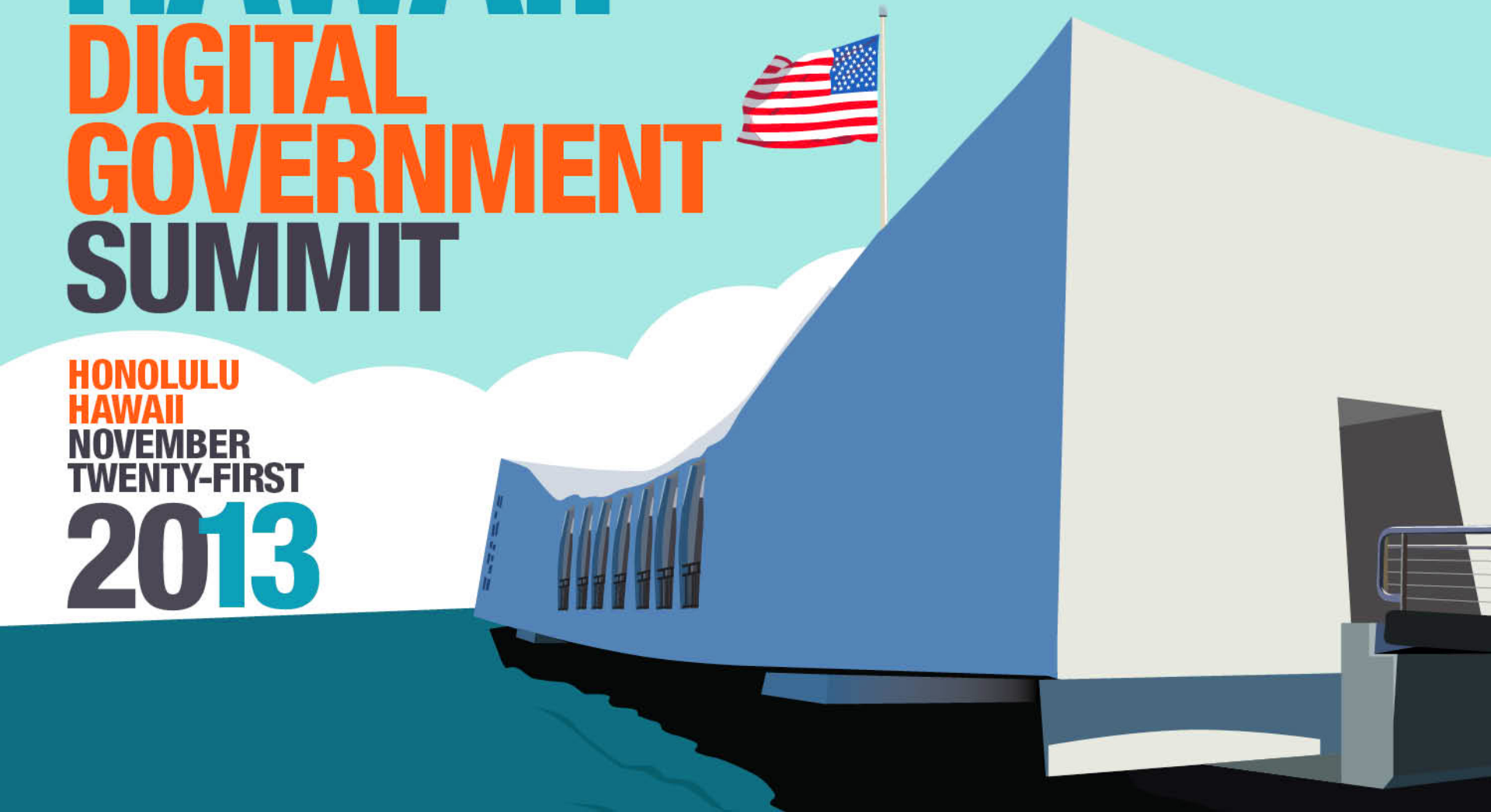
GOVERNMENT TECHNOLOGY®

HAWAII DIGITAL GOVERNMENT SUMMIT

HONOLULU
HAWAII
NOVEMBER
TWENTY-FIRST
2013

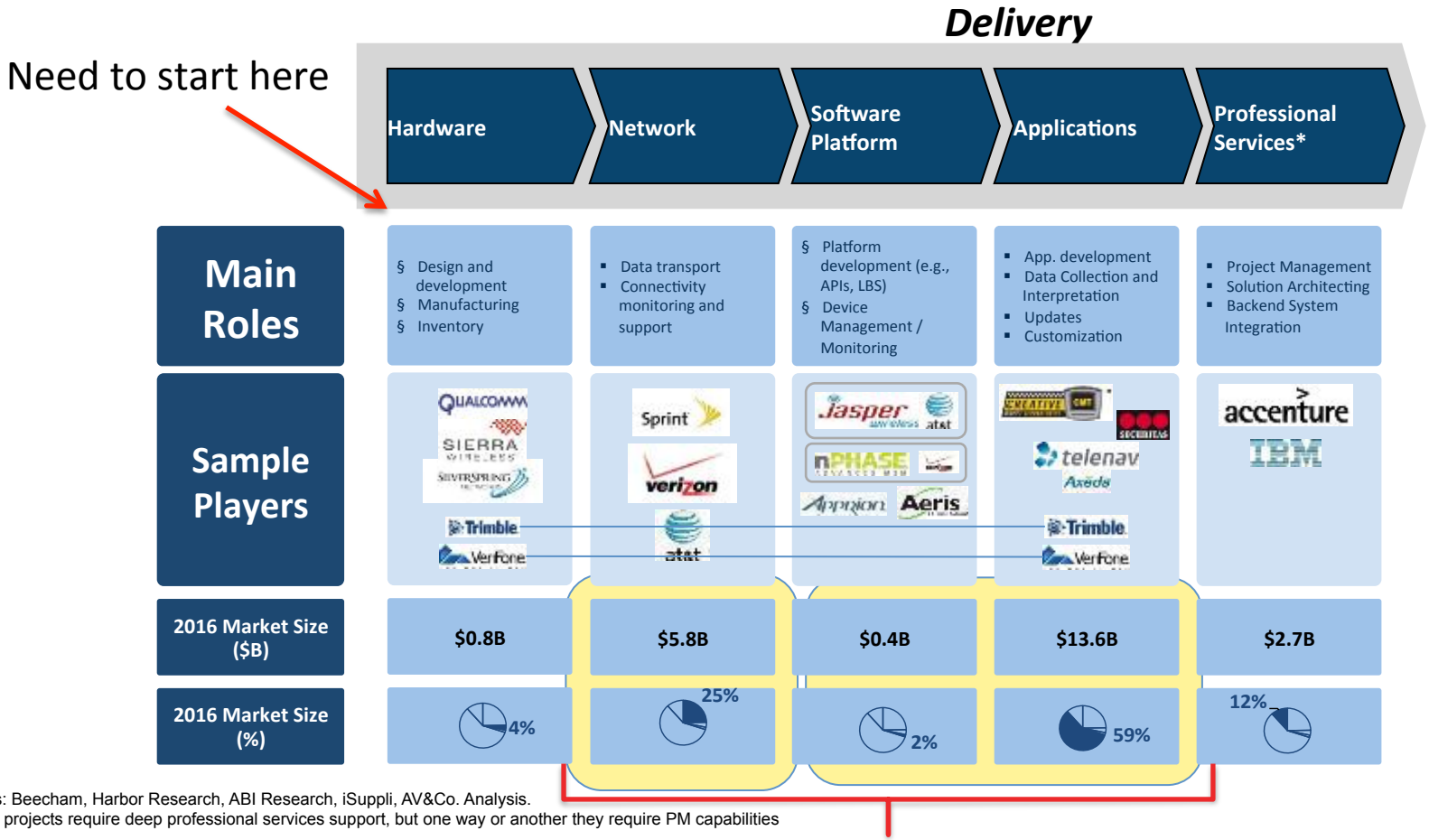


- **Session T6: The Internet of Things - Machine to Machine Technology**
- **Problem Statement**
  - Can trust ever be granted to an element from an untrusted source?
- **Alignment with State Transformation Plan**
  - Technology Transformation
  - Mobile Computing

- **Definition**
  - How do you secure a network of devices with multiple manufacturers, multiple users, multiple providers through multiple access.

- **Background**
  - Cisco IBSG (2011) predicts there will be 25 billion devices connected to the Internet by 2015 and 50 billion by 2020.
  - Out of the $23.3 Billion of the market in 2016, only 25% goes to network connectivity.

- The M2M value chain is fragmented with distinct sales and delivery responsibilities; out of the $23.3B of the market in 2016, only 25% goes to network connectivity
  - Approximately 60% of the market revenues go to application providers

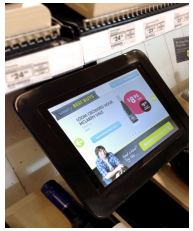


Sources: Beecham, Harbor Research, ABI Research, iSuppli, AV&Co. Analysis.
* Not all projects require deep professional services support, but one way or another they require PM capabilities

If you want to own of these delivery areas

Session T6: The Internet of Things - Machine to Machine Technology







Smart Phone Adoption

Connected Devices

Broadband Connectivity

New Ecosystem of Internet Application/Service Providers

"The 4 Quadrants"

- *Applications*
- *Services*
- *Network*
- *Devices*

Change adds complexity, requires detailed planning, and creates opportunities

It Takes a Network

Augmented Reality: Technology functions by enhancing one's current perception of reality. (Distortion)

- Virtual reality
- Image shifting
- Gaming, shopping

Versus

Reality, Augmented: Technology enhances reality without modifying the perception. (Amplification)

- Complex Adaptive Systems
- Vibration
- Health accumulation
- Human mechanization, information accretion

It Takes a Network

Trust can never be granted to an element from an untrusted source

HP and Calxeda's Moonshot ARM servers

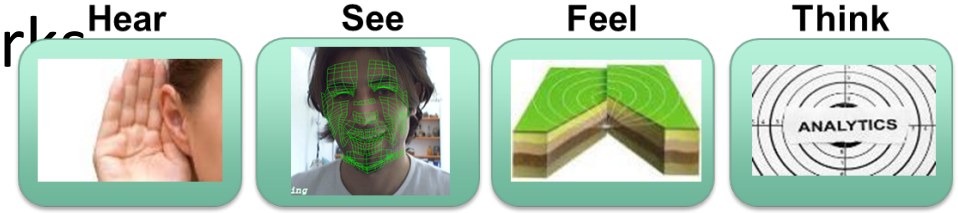
Zedboard

Trusted

It Takes a Network

- **Key Accomplishments**
  - Recognition that the network is the Data Center.
  - Evaluation of concepts like ARM's TrustZone

- **Summary**
  - Significant Opportunity
  - Transformative Thinking Creates Brilliant Networks

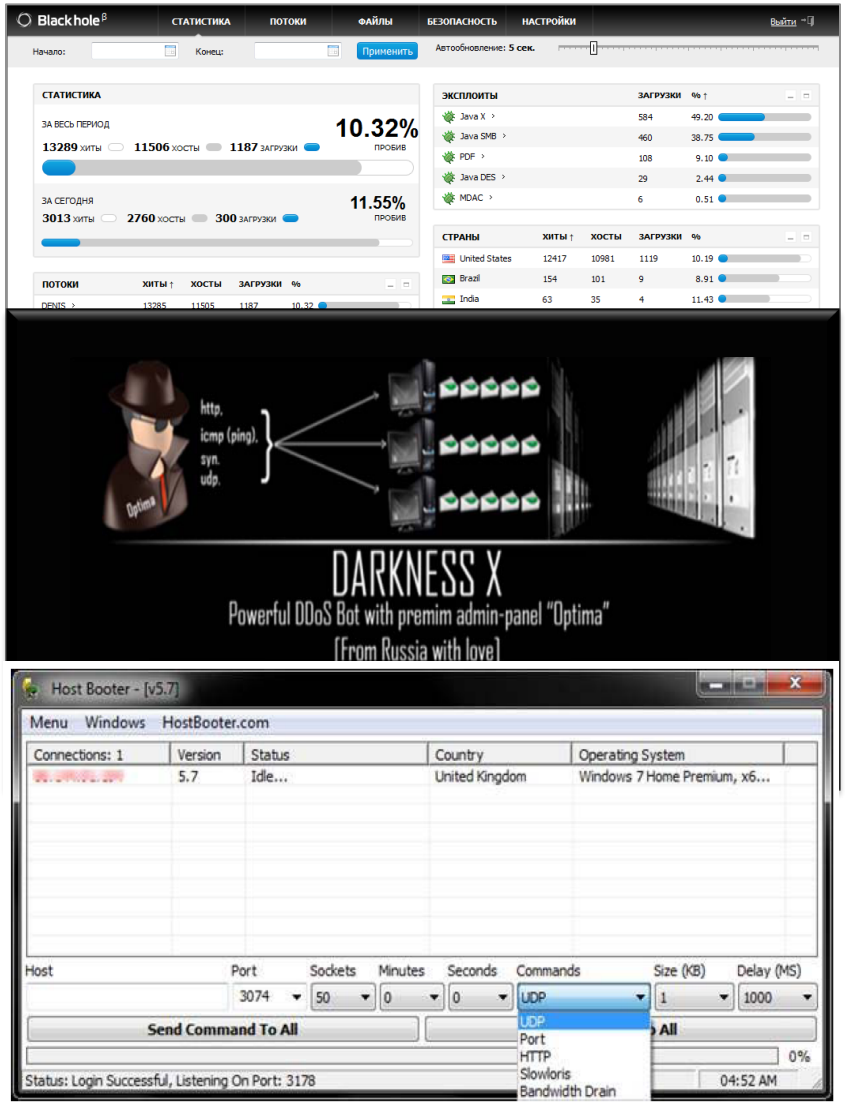


  - Bryan Ito, Business Sales Manager, Bryan.H.Ito@sprint.com, 808-779-5800

50 Billion Devices by 2020

You have to protect everything…
The bad guys only have to find ONE vulnerability

Cybercrime – it's a business

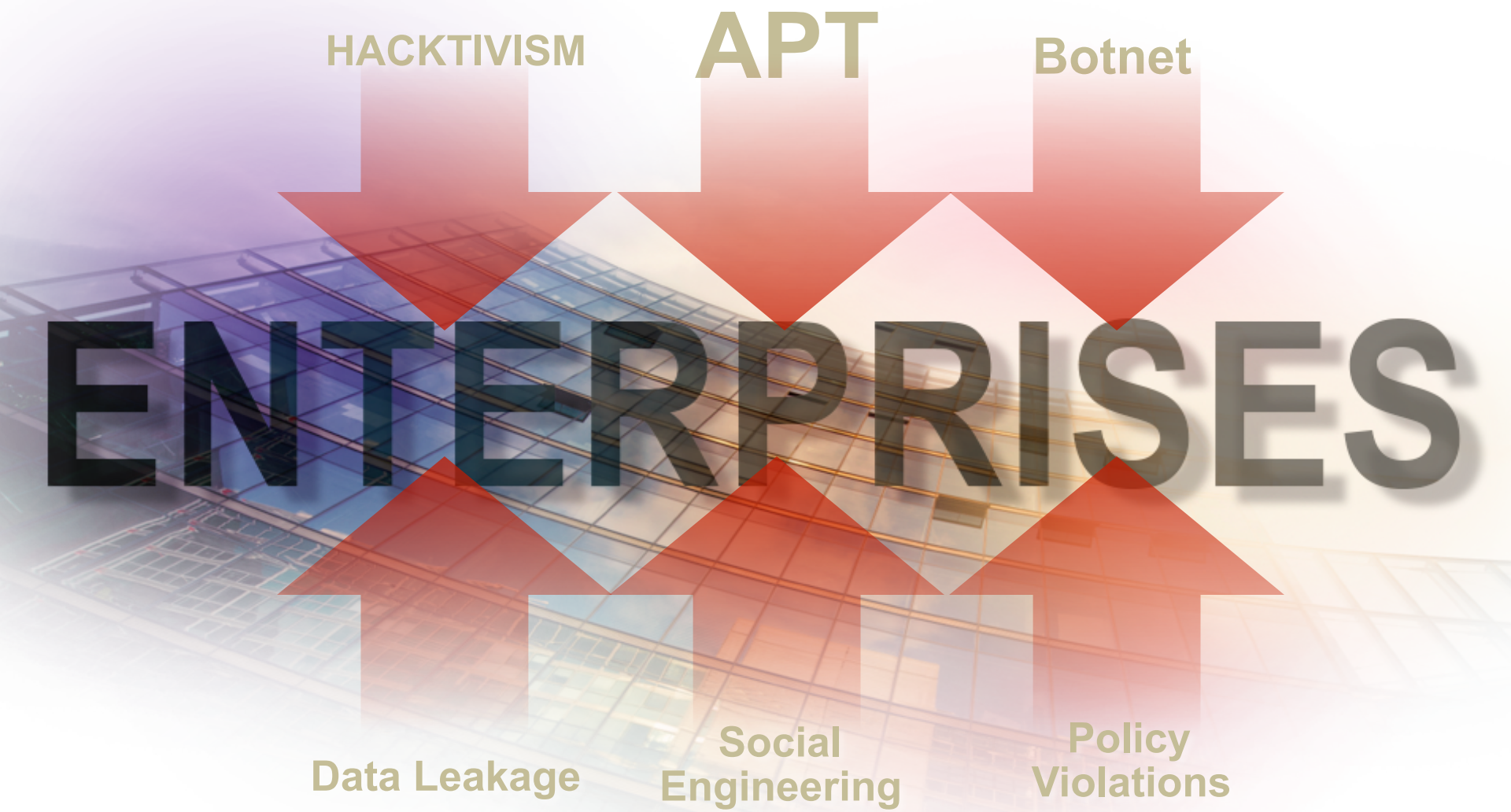


Blackhole exploit kit: a collection of many exploits which take advantage of vulnerabilities in web browsers

Darkness X – $450 DDoS Bot

Host Booter UDP/Port/HTTP/ Slowloris/ Bandwidth Drain attacks

IT’s a vulnerable world



Start with the basics….Define Trust

Authentication: Who and What are you?....CA for Machines, Applications and Processes.

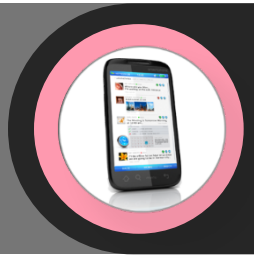
Authorization: Everything has a whitelist, graylist, and blacklist.

Audit: Monitor, Track, Report, and Correlate

Adaptive Trust Models…

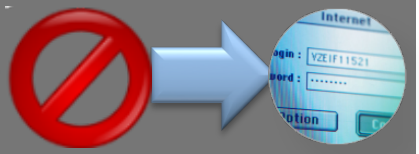
Multi-Layered Threat Prevention

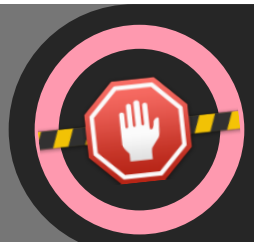
Check Point SOFTWARE TECHNOLOGIES LTD.



Identity

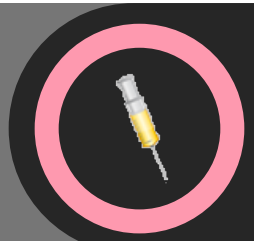
Identity based policy





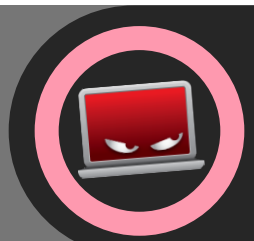
IPS

Stops exploits of known vulnerabilities



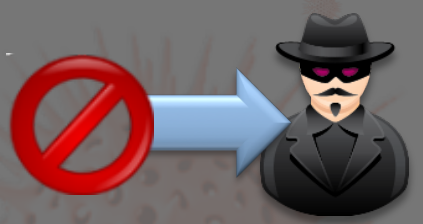
Antivirus

Block download of malware infested files



Anti-Bot

Detect and prevent bot damage



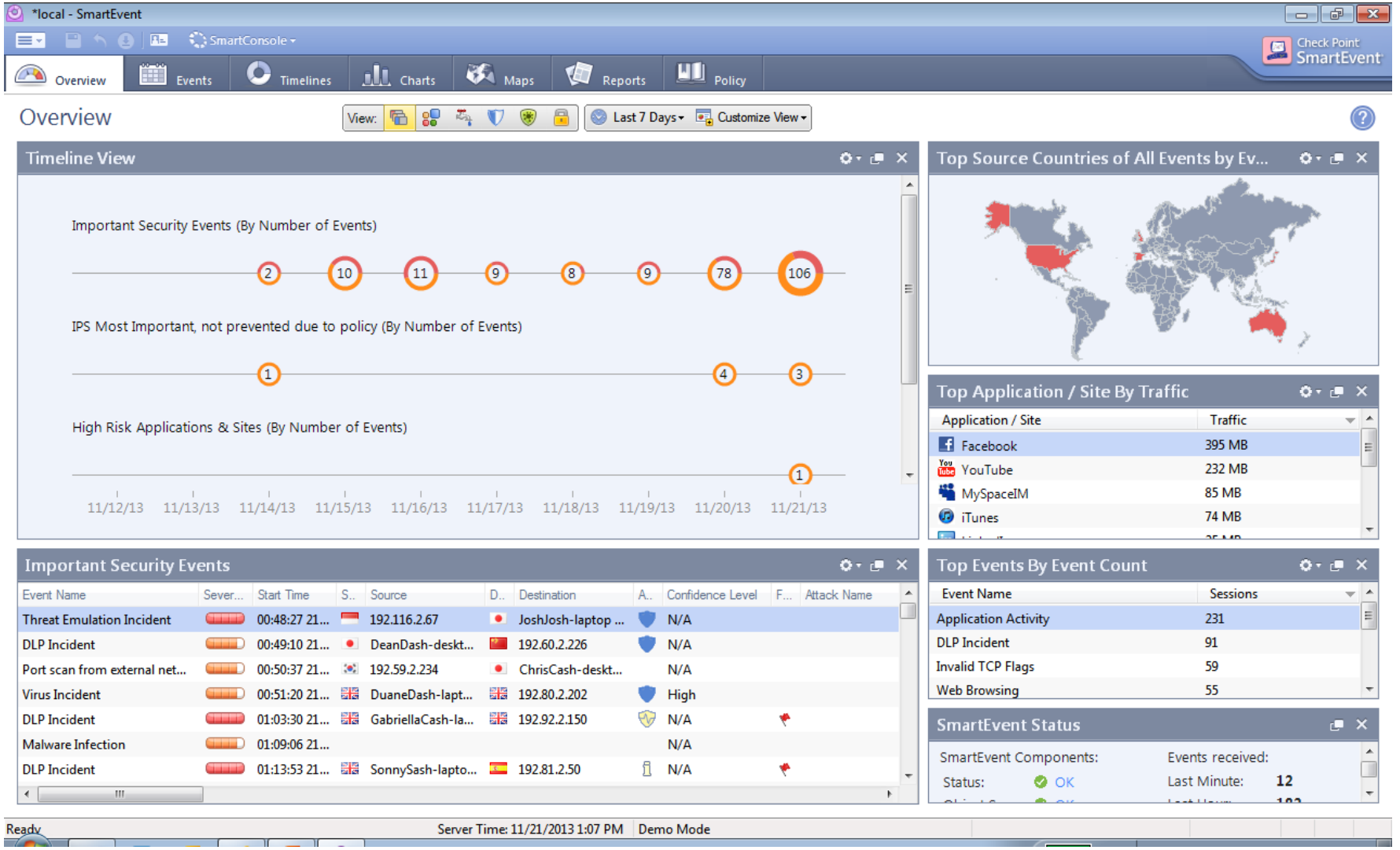
Real Time Threat Intelligence?

Global Threat Awareness and Guidance

Access to global security intelligence collaboration infrastructure delivering real-time protection to security gateways

- Reference Global Security Archive of Known Threats
- Global Application/Process Authority
- Malware communication monitoring and correlation

Security Oversight and Visibility?



UNIVERSITY of HAWAIʻI at MĀNOA
WILLIAM S. RICHARDSON
SCHOOL OF LAW

The Internet of Things: Machine-to-Machine Technology

Hawai ʻi Digital Government Summit
Hilton Hawaiian Village

Danielle M. Conway
Michael J. Marks Distinguished Professor of Business Law &
Director, University of Hawai ʻi Procurement Institute
Nov. 21, 2013

Fundamental Issues

- **Confidentiality**
  - ✓ Privacy
  - ✓ Data Ownership and Control
  - ✓ Use of Client Information During Business Development Efforts
- **Security**
  - ✓ Data Protection and Preservation
  - ✓ Electronic Signatures
  - ✓ Biometric and Webcam Authentication
  - ✓ Pre-server Upload Encryption

Fundamental Issues

- **Efficiency**
  - ✓ Cost Benefit Analysis
    - ◆Public, Community, or Hybrid Cloud (Cloud Bursting)
    - ◆Private Cloud (Hosted/Server Based/On Premises)
  - ✓ Multiparty Document Collaboration
  - ✓ Document Storage
  - ✓ Calendaring
  - ✓ Searchable Filing Systems
  - ✓ Financial Documents
- **Boilerplate Service Level Agreements**

Legislation Bearing on Cloud Computing

- No National Laws to Protect Privacy of Information Shared Online

- But, there is a patchwork of protection that includes:
  - Privacy Act of 1974 (Pub. L. 93-579, Dec. 31, 1974)
  - Family Educational Rights and Privacy Act of 1974 (Pub. L. 93-380, Aug. 21, 1974, 20 U.S.C. §1232g)
  - Right to Financial Privacy Act of 1978 (Pub. L. 95-630, Nov. 10, 1978, 12 U.S.C. §3401 *et seq.*)
  - Privacy Protection Act of 1980 (Pub. L. 96-440, Oct. 13., 1980, 42 U.S.C. §2000aa *et seq.*)
  - Electronic Communications Privacy Act of 1986 (Pub. L. 99-508, Oct. 21, 1986)

International Legislation Bearing on Cloud Computing

- **EU Directive on Personal Data Protection (95/46/EC of 24 October 1995)**
  - Provide individuals with a uniform level of protection in their personal data throughout all of the member states
  - Applies to the processing of personal data (identified or identifiable natural person or data subject)

- **EU Directive on Privacy and Electronic Communications (2002/58/EC of 12 July 2002)**
  - Right to privacy w/r/t processing of personal data in the electronic comm'ns sector
  - Ensure confidentiality and security of comm'ns and the related traffic data by means of public comm'ns networks and publicly available electronic comm'ns services.

- **EU Proposed Draft of Data Protection Reform (2013)**

- **Some Other Countries – NO PROTECTION!**

Cloud Computing Policy at the State and Local Government Level

- Haphazard and problematic
- No uniform system of procedures, regulations, or support exists.
  - Small municipality or county governments often lack the resources to effectively implement cloud computing on their own.
  - State and Local government organizations can be overwhelmed by unforeseen complications.
  - Example: Massachusetts State email system

Massachusetts State Email System

- Moving the state email system to a cloud service provider implicated privacy and security concerns at both the federal and state level.
- Federal
  - IRS tax information security guidelines
  - Social Security Administration's healthcare fraud and abuse data collection program
- State
  - Over 100 regulations governing privacy and data security
- State officials did not anticipate the complications that arose from compliance with the various federal and state regulations. As a result, both the expense and the time required to move the email system were much greater than originally estimated.

Cloud computing vendors offer several different infrastructure models to State and Local Government organizations

- Private Cloud

  The cloud computing platform is operated within the organization's firewall, and managed by the organization's IT department. It is the most secure option, but also the most resource intensive.

- Software as a Service (SaaS)

  The vendor hosts a software application for the organization on their cloud computing platform. It is frequently used for email hosting, and other similar applications.

- Infrastructure as a Service (IaaS)

  The vendor provides computing power, memory, and storage for the organization. It is often used for data storage or website hosting.

- Platform as a Service (PaaS)

  The vendor provides a cloud computing platform on which the organization can run numerous applications. It is a very flexible option, similar to the private cloud, but managed and maintained by the vendor.

Some States lead in implementing cloud computing infrastructure

- Maine
  - Uses the firm CGI to host financial and procurement applications, as well as HR management tools.
- Ohio
  - State IT department hosts email on a private cloud for state agencies and/or helps agencies set up their own in-house email hosting.
- Utah
  - Hosts email and provides cloud computing services to agencies, counties and municipalities.

Utah

- State maintains a private cloud
- Provides cloud computing services for all state agencies
  - Email hosting
  - Data storage
- Offers email and data storage services to county and municipal governments.
  - State services are not compulsory. Counties and municipalities may choose to invest in private clouds.
- State cloud service caters to small cities that lack the capital to set up their own cloud infrastructure.

County and Municipal Government

- County and municipal cloud infrastructure varies widely based on the needs of the individual communities.
- Miami, Florida
  - Uses Microsoft data centers to host its 311 nonemergency response application.
- Sussex County, New Jersey
  - Hosts email, data storage, and applications on a private cloud, both for the county itself and for the towns within the county.
- Somerset County, Maine
  - Hosts public safety applications on a private cloud. A neighboring county also uses Somerset County's cloud computing infrastructure.

Somerset County, Maine

- The County maintains a private cloud, and hosts public safety applications for law enforcement and fire departments.
  - 911 emergency service
  - Records management
  - Jail management
- Somerset County has expanded its cloud infrastructure to serve neighboring Franklin County.

  Several Franklin County police and fire departments already rely on Somerset County's cloud-based public safety applications, and more departments are considering adopting it.

Risk Management

- Avoid Boilerplate; negotiate terms of service/use of Cloud Computing Platform (SaaS)
- Review and update privacy policies
- Draft Express Language in Retainer Agreements About Confidentiality and Security of Client Data and Information
- Be aware of industry best practices
- Maintain E&O Insurance, with express coverage for compromises in data
- Run Cost Benefit Analysis of free v. paid cloud services

Strategies & Best Practices

- Conduct Due Diligence in the following:
  - Selecting a Service Provider
  - Selecting a Platform
- Establish a Client Advisory Board
- Keep Clients Informed
- Err on the Side of Disclosure to Clients
- Negotiate Terms of Use/Service, especially remedies in the event of crashes, breach, corruption, business interruption, or destruction
- Investigate the Potential for Cloud Computing Partners (as opposed to service providers), possibly under a Community Cloud Model

Questions?